Encryption Wizard 3.2
User Guide

ATSPI Technology Office
Air Force Research Laboratory

Last Updated: 1 June 2011

For EW versions >= 3.2.10

Table of Contents

1. General Information

Encryption Wizard is a Java-based file encryption program that can be used to quickly and easily encrypt sensitive files. It is an easy to use tool for protecting sensitive (but not classified) documents[1], and for protecting files before transmission via email. It allows a user to encrypt files using a 128-bit implementation of the Advanced Encryption Standard (AES) with simple drag-and-drop efficiency.

Encryption Wizard can significantly increase an organization's security posture at little to no cost to protect sensitive data in transit (E-mail, FTP, or shared web folders) or at rest on a removable storage device. The primary version for government users utilizes a FIPS 140-2 validated encryption engine licensed from RSA Security.

2. System Requirements

- Any operating system capable of running the Oracle Java Runtime Environment (e.g.: Windows, Linux, MacOS).
- Oracle Java Runtime Environment (JRE) 1.5 or greater. Encryption Wizard is often distributed on a CD-ROM that contains a copy of the most current version of the JRE, which can also be downloaded from http://www.java.com.

PLEASE NOTE:	Oracle does not currently support smart cards via the PKCS#11 interface on 64-bit Microsoft Windows systems; this means that EW does not currently support CAC/PIV on Windows x64 editions. See section 2.1 of the following for details: http://download.oracle.com/javase/6/docs/technotes/guides/security/p11guide.html#Requirements

3. Recommended Use

The AFRL/RY ATSPI Technology Office recommends the use of this tool for the protection of all sensitive data when in transit or at rest.

4. Installation and Setup

Encryption Wizard requires no installation or setup process. Assuming that a recent version of Java is installed on a user's system, Encryption Wizard may be executed simply by double-clicking on the executable, `wizard-3.2.10{-FIPS}.jar`. On Microsoft Windows, there are user convenience features that associate the Encryption Wizard file types with the tool and a Send To context menu as well (see Section 6.3 for details).

[1] Encryption Wizard is approved for use on some classified networks for enforcing need-to-know within the network. EW ***has not*** been certified to render classified materials as unclassified when encrypted.

5. Using Encryption Wizard

5.1. *Launching Encryption Wizard*

Encryption Wizard can be accessed either through the command line in Windows or Linux, or by double clicking on the Encryption Wizard `.jar` file.

From a File Explorer window

1. Browse to the directory that contains the Encryption Wizard file
2. Double click on `wizard-3.2.10.jar`

From a command prompt

- Change directory (`cd`) to the directory holding the JAR file and type:

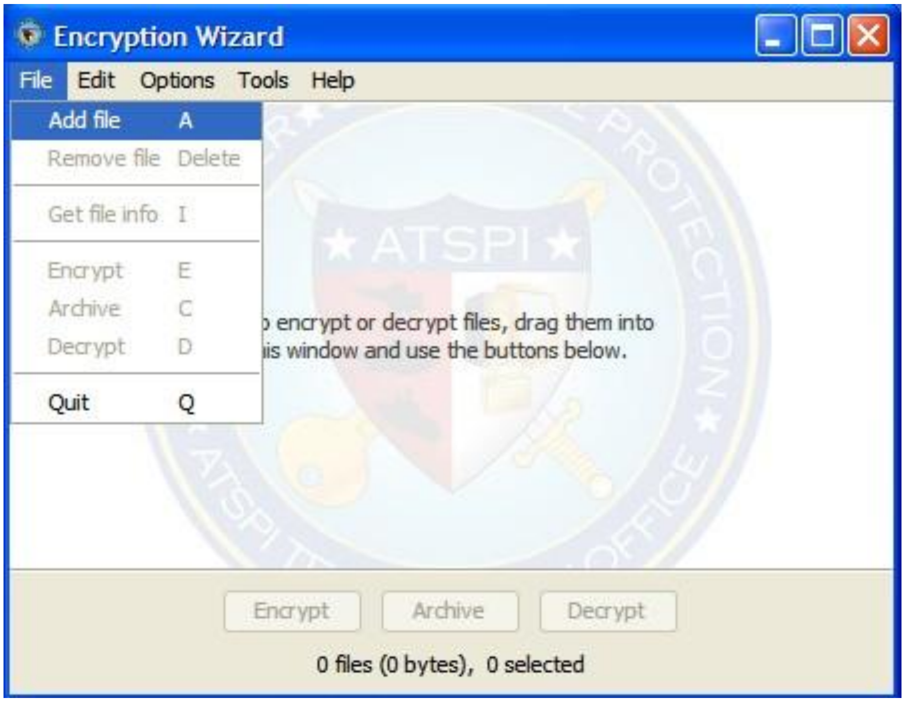
```
java -jar wizard-3.2.10.jar
```

5.2. *Encrypting a File*

Selecting a File to Encrypt

To encrypt files, open Encryption Wizard and add a file to the main file list in one of the following ways:

- Drag and drop file(s) to the file list window (middle of application - see Figure 1)
- Use the menu to select "Add File", choose file(s) from the file selection dialog
- Press 'a' to bring up the file selection dialog



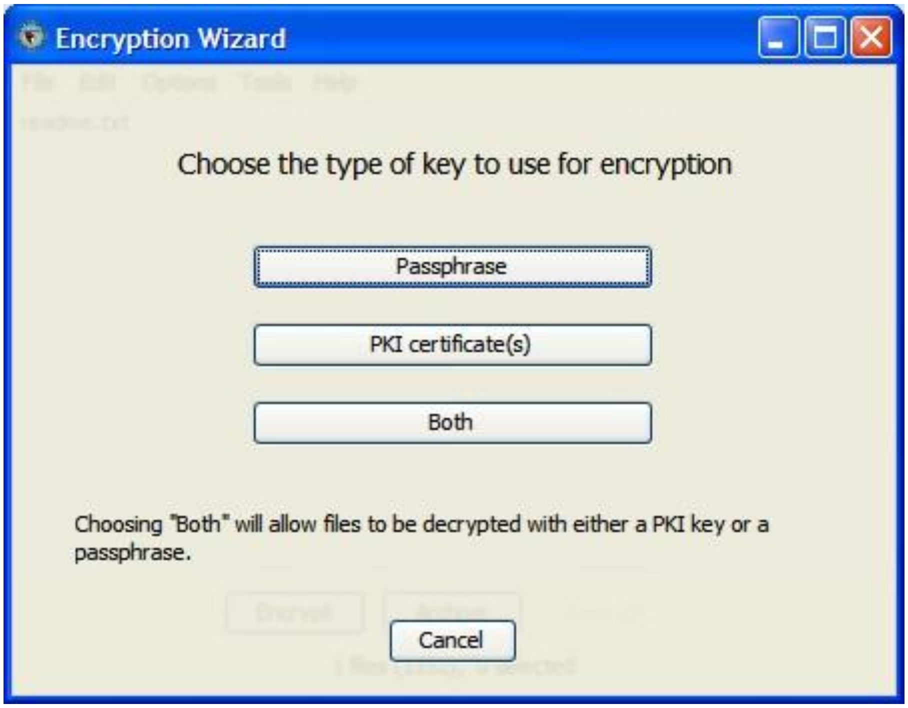
o encrypt or decrypt files, drag them into
is window and use the buttons below.

0 files (0 bytes), 0 selected

Figure 1: Encryption Wizard User Interface

Selecting the Key Type

1. Once the file is in the file list, select the file(s) to encrypt and click the "Encrypt" button in the bottom tool bar (lower left inside Figure 1) – OR – press 'e'. If no files in the file list are selected, all files in the file list will be encrypted.
2. Select the key type by selecting: passphrase, Public Key Infrastructure (PKI) Certificate, or both (see Figure 2)



Choose the type of key to use for encryption

Choosing "Both" will allow files to be decrypted with either a PKI key or a passphrase.

Figure 2: Choose a Key Type

Encrypting with a Passphrase

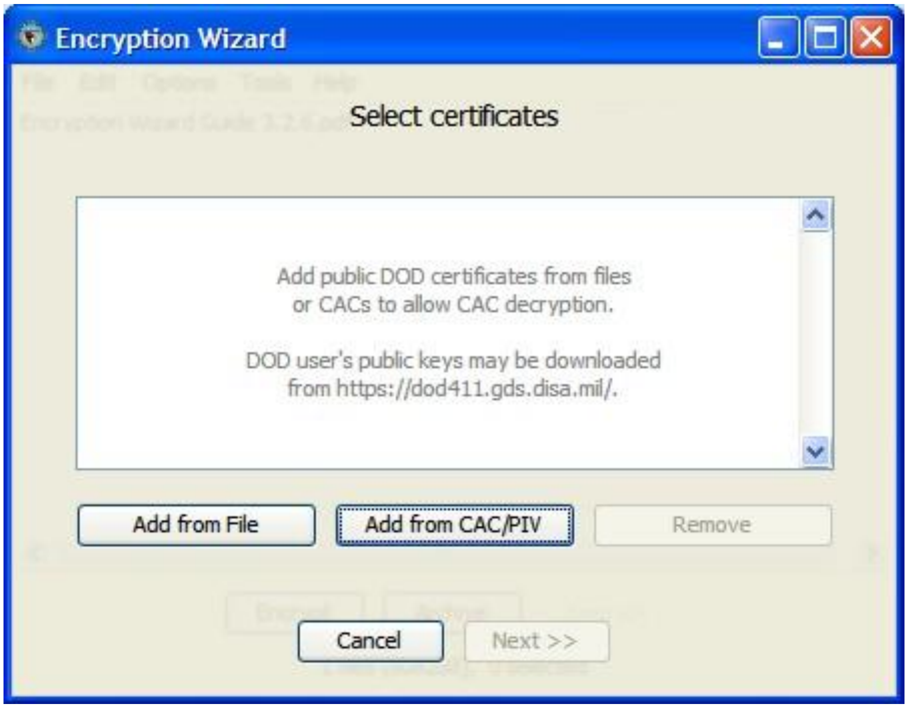
- Enter and confirm the passphrase, then select 'Encrypt>>' or press 'Enter'.
- After the file is encrypted, the user will be asked if they wish to delete the original file (this behavior is user selectable, see Section 6.4). The file is now safe to send over the Internet or store on one's portable media/computer.

NOTE:	Be sure to select a memorable passphrase – or record it out-of-band (e.g. Write it down and put it in a safe place). *Encryption Wizard does not have a key escrow or master key feature – if the passphrase is* ***lost****,* ***forgotten****, or* ***mis-entered****, the data* ***cannot*** *be decrypted.*
NOTE:	When encrypting a file to share with someone else, choose a passphrase that can be shared – **do not use** a personal computer or network login password or other sensitive personal passphrase.
NOTE:	Encryption operations are irreversible without the original keying material (passphrase or PKI certificates) – make sure to either keep a copy of the passphrase or of the original data. If it is possible to encrypt with a PKI public key, consider using it as a backup to a lost password.

Encrypting with PKI Certificate(s)

A user may select PKI Certificates two different ways. First, PKI Certificates can be read from a smartcard (e.g.: CAC or PIV). Insert the smartcard into the reader and enter the Personal Identification Number (PIN) when asked for it. Choose the Encryption Certificate. Second, multiple public key certificates can be read from public key certificate files (.cer). The files can be added by either dragging the files into the window or by selecting the "Add from File" button (see Figure 3). A user can encrypt a file with the public key certificates of every member of a team to create a file that can only be read by team members. Public key certificates for DoD team members can be located and downloaded from https://dod411.gds.disa.mil. A user may use public key certificates from both a smartcard and from public key certificate files.

NOTE:	When using the DoD CAC, ***always*** use the Encryption Certificate – this is the only certificate that is kept in escrow by DISA for later retrieval. If you encrypt your data with any other certificate, you may not be able to decrypt the file if you have been issued a new CAC.
NOTE:	If the file is encrypted with only a third party's PKI certificate, then ***only*** the holder of that PKI certificate will be able to decrypt the file. **For example:** If a file is encrypted with only the PKI certificate of the Secretary of Defense, then only the Secretary of Defense can decrypt the files. If you want to be able to decrypt the file, you will need to add your own public key.



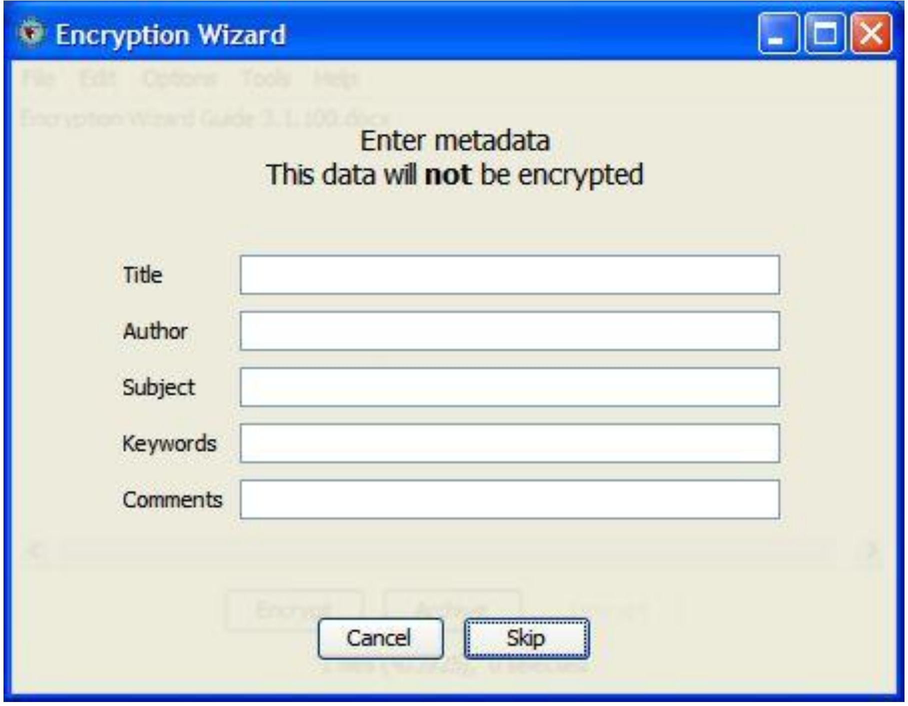
Add public DOD certificates from files or CACs to allow CAC decryption.

DOD user's public keys may be downloaded from https://dod411.gds.disa.mil/.

Figure 3: Select PKI Certificates

Adding File Metadata

After providing the PKI information and/or passphrase, Encryption Wizard now optionally requests searchable metadata on the encrypted file. The user supplied metadata (see Figure 4) is stored inside the encrypted file in cleartext so that it may be indexed by enterprise search tools. If you have installed Encryption Wizard and do not plan to use the metadata functionality, you may configure Encryption Wizard to suppress the display of the metadata dialog.



Enter metadata
This data will **not** be encrypted

Figure 4: Metadata enables search of encrypted content

5.3. *Decrypting a File*

The process for decrypting a file with Encryption Wizard is similar to the process for encrypting it. Simply add an Encryption Wizard file (a file with the extension .wzd) to the file list by dragging and dropping it, pressing ‘a,’ or selecting “File→Add File” from the menu. (Once Encryption Wizard is “installed” [see section 6.3, *Associating the .wza and .wza file extensions*], the user may also double-click on the file in Windows.)

- Once the file is in the Encryption Wizard file window, select the file and press the ‘Decrypt’ button. Encryption Wizard will ask for the keying material that was used to encrypt the file.
- If the file was encrypted with PKI, select a PKI source – either a private key PKI file or a smartcard; if it was encrypted with a passphrase, select “Passphrase” (see Figure 5).
- If the file was encrypted with PKI, follow the prompts from the smartcard middleware or unlock the private key PKI file.
- If the file was encrypted with a passphrase, enter the passphrase, and press “OK” or hit ‘Enter’ or ‘Return’.
- If the file was encrypted with both PKI and a passphrase, use the decryption method that is most convenient.

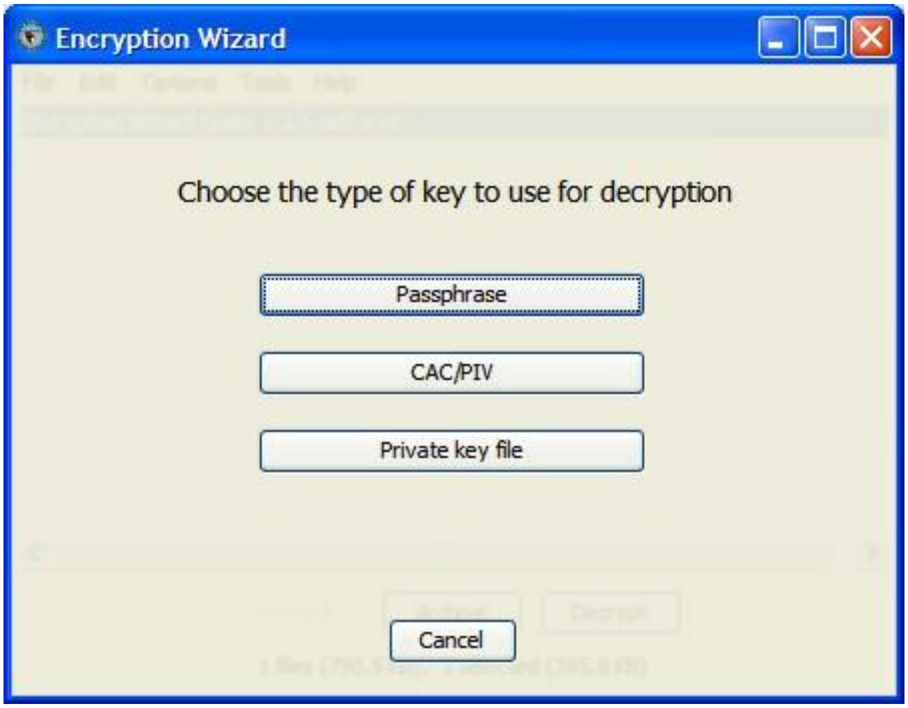


Figure 5: Choose a Decryption Key Type

The original file will be decrypted and restored to the original filename and extension.

5.4. *Encryption Wizard Archives*

Encryption Wizard supports the ability to create encrypted and optionally compressed file archives. Encryption Wizard Archives are similar to WinZip or other file archive utilities, except that they are secured by strong encryption. Encryption Wizard Archives are good for retaining backups of sensitive information on media that cannot or does not have to be physically secured.

Selecting Files for an Archive

To select files to archive:

- Drag and drop file(s) to the file list window (middle of application - see Figure 1)
- Use the menu to select "Add File", choose file(s) from the file selection dialog
- Press 'a' to bring up the file selection dialog

Creating an Archive

Name the archive by entering a filename; a user may also optionally select a path for the archive using the "Browse…" button. Compression is enabled by selecting the "Compress" checkbox (see Figure 6). The encrypted archive file is given a '.wza' file extension (e.g.: `filename.wza`).

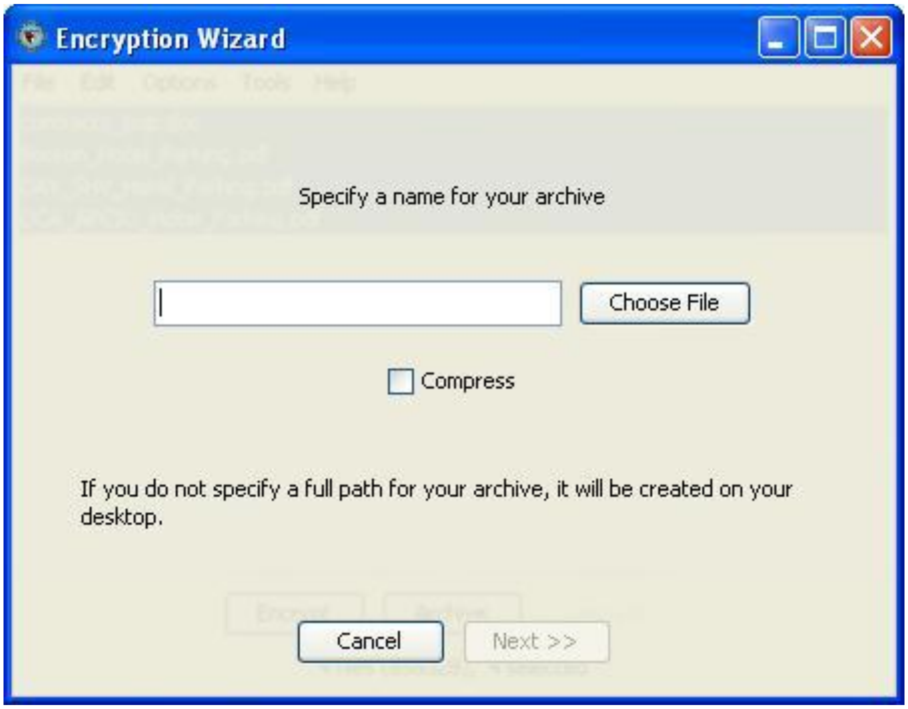

Encryption Wizard
Specify a name for your archive
Choose File
□ Compress
If you do not specify a full path for your archive, it will be created on your desktop.
Cancel
Next >>

Figure 6: Creating an Encryption Wizard Archive

Selecting the Keying Material for an Archive

Keying material for Encryption Wizard Archives are selected in the same manner as other Encryption Wizard files, see Section 5.2 for more details.

Expanding the Archive

Once a user opens Encryption Wizard and selects the archive(s) to expand, select the “Expand” action (see Figure 7).

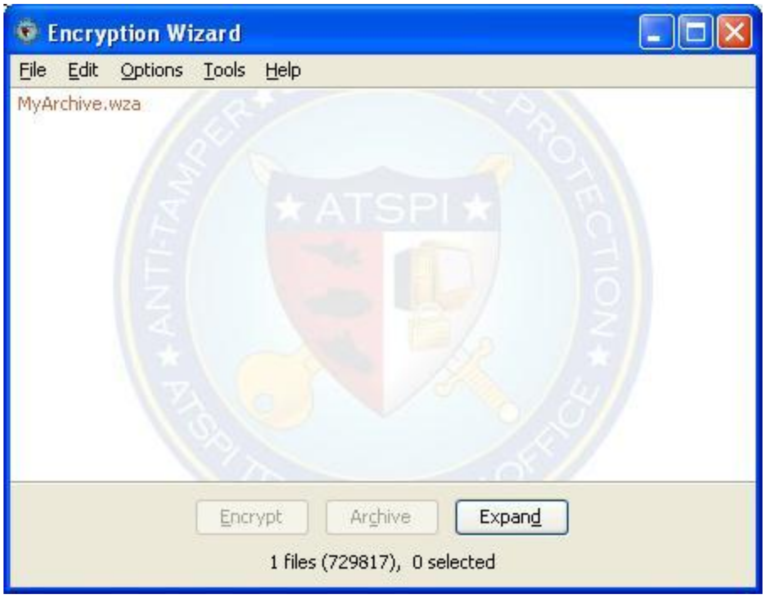
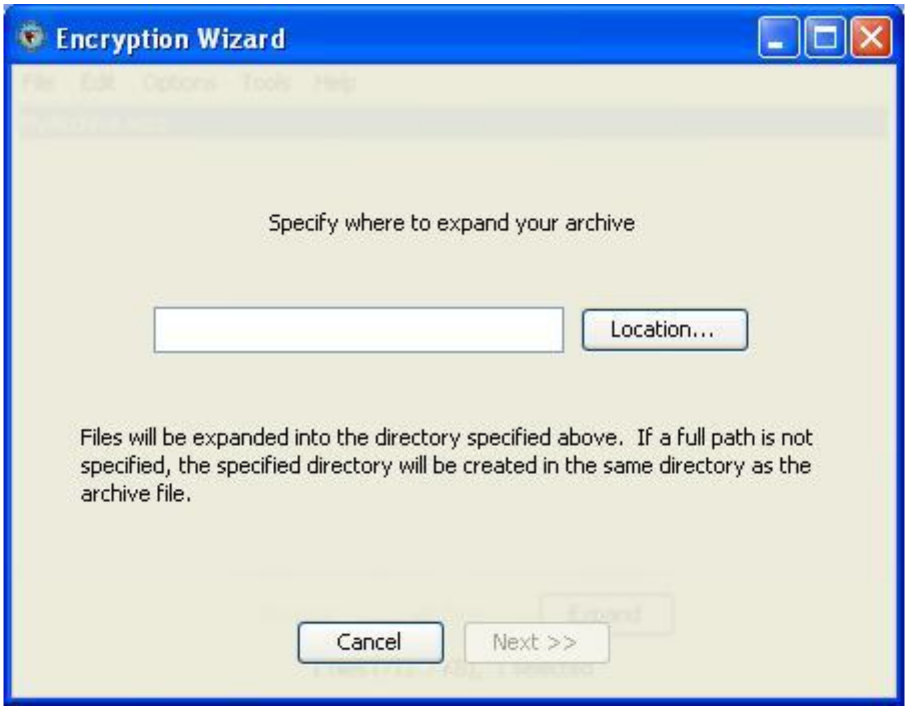


Figure 7: Choosing an Encryption Wizard Archive to Expand

Next, specify the directory in which to expand the archive (see Figure 8). Selecting “Next >>” expands the archive to the specified directory.



Specify where to expand your archive

Files will be expanded into the directory specified above. If a full path is not specified, the specified directory will be created in the same directory as the archive file.

Figure 8: Expanding an Encryption Wizard Archive

Key material selection is the same as for an encrypted file, see Section 5.3.

6. Additional Features and Options

Encryption Wizard has additional features that make encrypting files and data easier to accomplish.

6.1. Hotkeys

Hotkeys provide a quick way to access the main features of Encryption Wizard. To use a hotkey, simply type the hotkey while the Encryption Wizard window is the active window:

a	Add files to the file list
r	Refresh files in the file list
e	Encrypt selected unencrypted files in the file list
d	Decrypt selected encrypted files in the file list
c	Archive the selected files in the list
l	Access the Encryption Wizard log
Del	Remove selected file(s) from the file list
F1	Access the help system
Ctrl-A	Select all the files in the file list
Esc	Deselect all files in the file list

6.2. Command Line Options

Encryption Wizard has command line counterparts for most GUI operations. The command line interface may be used to encrypt files, decrypt files, and to create archives.

The general command line format is as follows. All operations and options must start with a '-' (hyphen).

```
java -jar wizard3.jar [operation] [options] FILE1 FILE2 ...
```

Only a single operation may be specified. If no operation is supplied, an Encryption Wizard window will be opened and its file list will be populated with any files specified on the command line. Possible operations are:

`h`	Print a help message that lists available options and operations
`e`	Encrypt files
`d`	Decrypt files
`a ARCHIVE_NAME`	Create an archive named `ARCHIVE_NAME`
`x DEST_PATH`	Expand an archive to the path `DEST_PATH`
`s`	Let Encryption Wizard guess what to do based on the input file types

Multiple options may be specified. Possible options are:

`c`	Enable compression
`p PASSPHRASE`	En/decrypt with passphrase `PASSPHRASE`
`v`	Enable verbose logging

The user may select one of the following operations to perform: encryption, decryption, archive creation, or archive expansion. The archive functions require a path argument to tell Encryption Wizard either what the name of the archive file should be, or where to store files that are expanded from an archive.

6.3. Associating the .wzd and .wza file extensions

(The following features are limited to Microsoft Windows.) A user can associate the .wzd and .wza extensions with Encryption Wizard. This will allow Windows Explorer to display a special icon for Encryption Wizard files, and allow Encryption Wizard to be executed when a .wzd or .wza file is double-clicked. This feature also adds Encryption Wizard as a “Send To” destination (access “Send To” by right-clicking on a file in Explorer).

To associate Encryption Wizard to its file types and add it to the list of "Send To" destinations:

- From the toolbar, select 'Tools'
- Select 'Install'

NOTE:	This feature does not currently work with the FDCC/SDC unless the user is an administrator. However, the registry changes needed to achieve these effects could easily be pushed out across an enterprise. Please contact the ATSPI Technology Office for details.

6.4. Selectable Options

Encryption Wizard includes a number of configuration options that will be stored in the user's application preferences directory. Figure 9 illustrates these options.

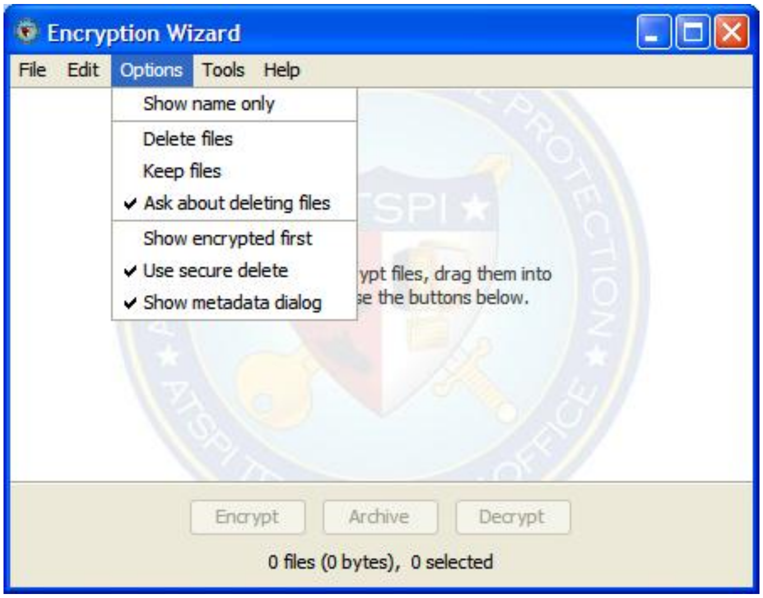


Figure 9: Selecting configuration options

6.4.1. Selecting the default encryption/decryption behavior

Versions of Encryption Wizard prior to 3.1.100 would encrypt and decrypt files "in place" – if a file was encrypted, the original unencrypted file was deleted; conversely, if a file was decrypted, the originally encrypted file was deleted. This option was added to permit the user to select one of three options:

- Always delete the original form of the file (default behavior for versions < 3.1.100)
- Always keep files
- Always ask about removing the original form of the file (default behavior for versions > 3.1.100)

Figure 9 illustrates the implementation of this option.

6.4.2. Selecting the default file deletion behavior

Versions of Encryption Wizard >=3.2.4 include the option for performing a more secure delete. The method used is specified in *DoD 5220.22-M National Industrial Security Program Operating Manual*, February 1995, Section 8-501.d.1, and consists of overwriting all file locations three (3) times: first time with a character, second time with its complement, and the third time with a random character. Figure 9 illustrates the selection and implementation of this option.

6.4.3. Disabling the metadata request dialog

Version 3.2.9 adds the ability to disable the metadata request dialog (see Adding File Metadata on page 7 and associated Figure 4).

6.5. Optional Key Escrow

Encryption Wizard also supports optional key escrow. The key escrow feature permits enterprises to embed a PKI key of their choosing into every file created by Encryption Wizard in their organization. This would permit the organization to recover encrypted data in the event that the original passphrase and/or PKI keys were lost or otherwise unavailable. This capability is referred to as "Encryption Wizard – Enterprise Edition". As of this writing, this feature must be enabled by the ATSPI Technology Office, see contact info in Section 8.

7. Licensing

Encryption Wizard is available in two forms: one that includes a FIPS 140-2 validated encryption engine (EW-Govt) and another that relies on the encryption capabilities native to a user's Java Runtime Environment (EW-Public).

The FIPS 140-2 validated version of Encryption Wizard contains a cryptographic module licensed from RSA®. The FIPS version may only be executed by US Government employees or contractors under contract with the US Government and is for use on data for official government use. It may only be distributed by ATSPI and by designated ATSPI distribution authorities. Users may NOT examine code contained in the RSA licensed cryptographic module contained in the FIPS version.

Information regarding RSA's FIPS 140-2 validation may be found here: http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140val-all.htm#820

8. Obtaining Support

Encryption Wizard support is available by contacting the ATSPI Outreach office.

AFRL/RY ATSPI Technology Office
ATSPI_Outreach@wpafb.af.mil
http://spi.dod.mil

Appendix A – Obtaining copies of your old (escrowed) CAC certificates to decrypt old files

NOTE:	This documentation is supplementary and is not fully tested across the DoD

This document describes how to obtain expired or retired personal DoD PKI certificates from the escrow facilities at DISA, and use them to open files encrypted with the older PKI certificates with Encryption Wizard.

Summary of steps:

1. **Obtain older PKI key from escrow**
2. **Prepare key for use with Encryption Wizard**
3. **Use with Encryption Wizard**

1. Obtaining personal DoD PKI certificates

There is both an automated and manual process. Full instructions and assistance can be received from your agency/service PKI helpdesk. Follow directions here[2]: https://afpki.lackland.af.mil/html/keyrecovery.cfm

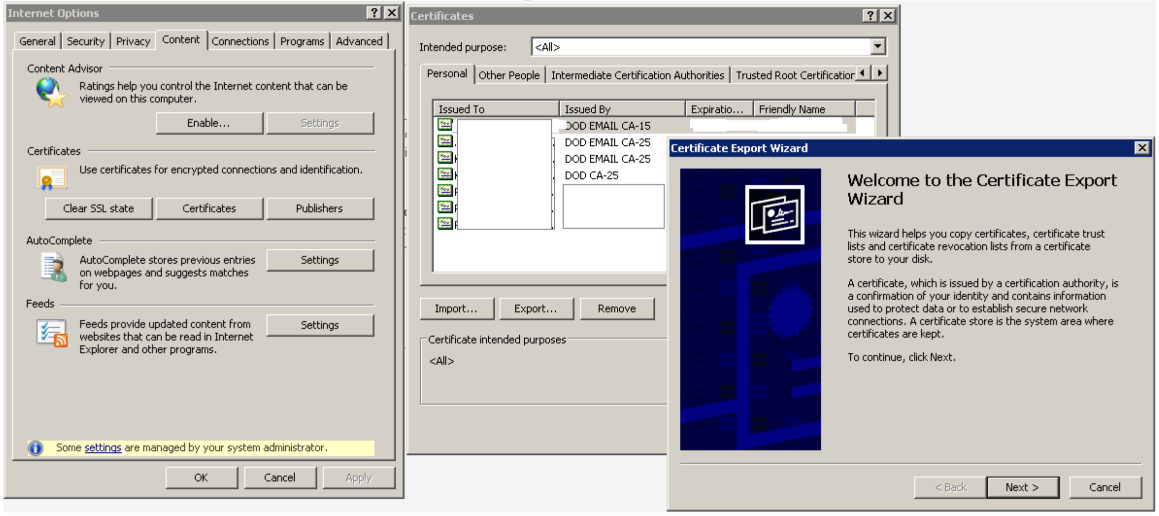
2. Preparing an escrow certificate for use with Encryption Wizard

Due to a bug either in Encryption Wizard or with the escrow certificates, you must first import the escrow key into Internet Explorer, and then export it into PKFX format to use it with Encryption Wizard.

2.1. Follow these instructions provided by the Air Force PKI Office to import the certificate into Internet Explorer (steps 12-22 of https://afpki.lackland.af.mil/assets/files/CI-07-02-002_Automated_E-mail_Encryption_Key_Recovery_QRG_V1100.doc)

2.2. Export the Certificate from Internet Explorer to PFX format

2.2.1. Open IE; Select Tools->Internet Options; click Content tab; click Certificates; Select escrowed certificate; Select export



Ratings help you control the Internet content that can be viewed on this computer.

Use certificates for encrypted connections and identification.

AutoComplete stores previous entries on webpages and suggests matches for you.

Feeds provide updated content from websites that can be read in Internet Explorer and other programs.

Some settings are managed by your system administrator.

Issued To	Issued By	Expiratio...	Friendly Name
	DOD EMAIL CA-15		
	DOD EMAIL CA-25		
	DOD EMAIL CA-25		
	DOD CA-25		

Welcome to the Certificate Export Wizard

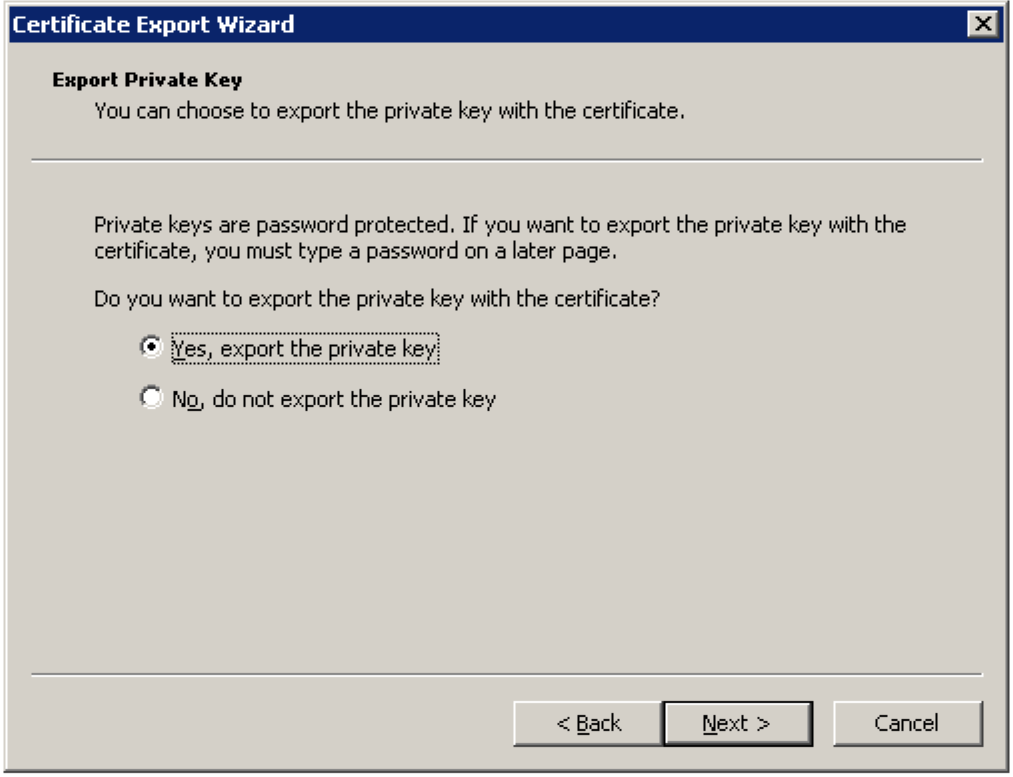
This wizard helps you copy certificates, certificate trust lists and certificate revocation lists from a certificate store to your disk.

A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

To continue, click Next.

[2] Since AFRL is an Air Force unit, the following instructions reference instructions from the Air Force PKI office. They are provided in the hope that they will be of assistance to you.

2.2.2. Export Private Key? YES



Export Private Key

You can choose to export the private key with the certificate.

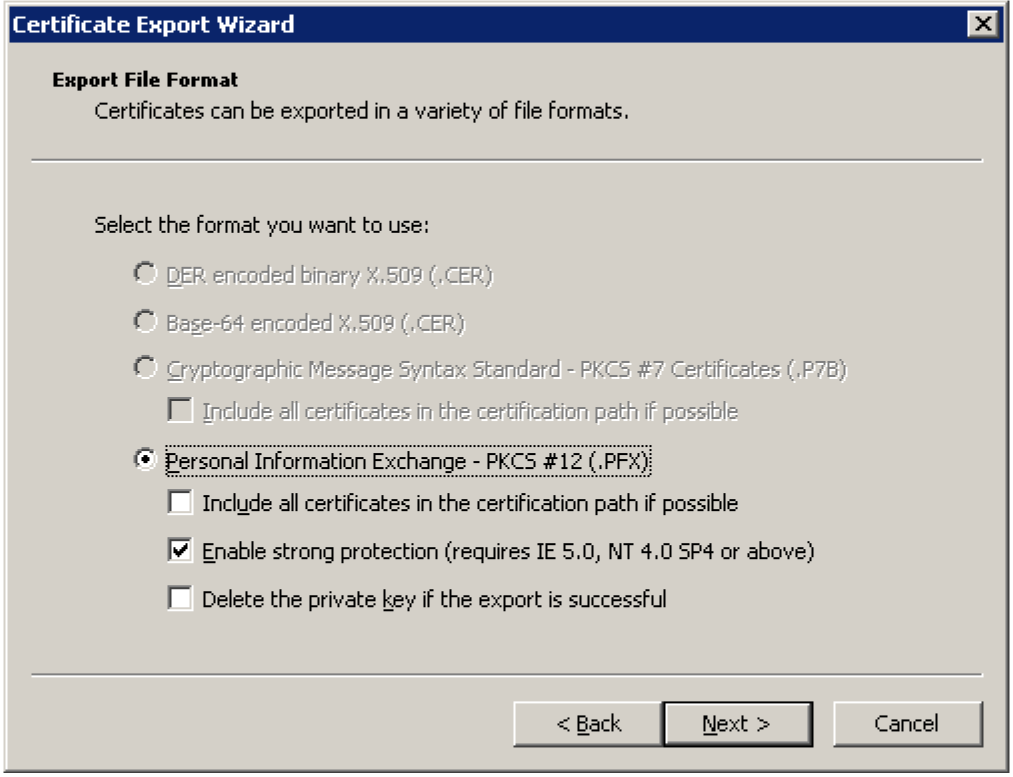
Private keys are password protected. If you want to export the private key with the certificate, you must type a password on a later page.

Do you want to export the private key with the certificate?

● Yes, export the private key

○ No, do not export the private key

2.2.3. Save as PFX file – use options as shown



Export File Format

Certificates can be exported in a variety of file formats.

Select the format you want to use:

○ DER encoded binary X.509 (.CER)

○ Base-64 encoded X.509 (.CER)

○ Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B)

□ Include all certificates in the certification path if possible

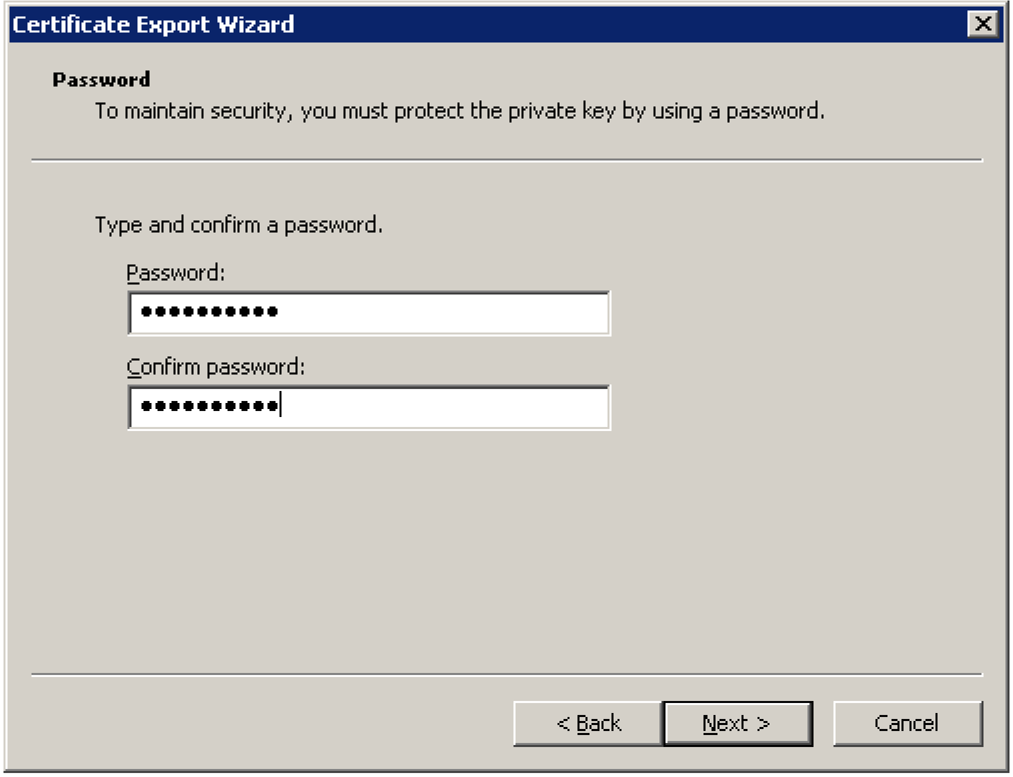
● Personal Information Exchange - PKCS #12 (.PFX)

□ Include all certificates in the certification path if possible

☑ Enable strong protection (requires IE 5.0, NT 4.0 SP4 or above)

□ Delete the private key if the export is successful

2.2.4. Choose a password – it can be the same as the 16-character one from DISA or a unique one



Certificate Export Wizard

Password

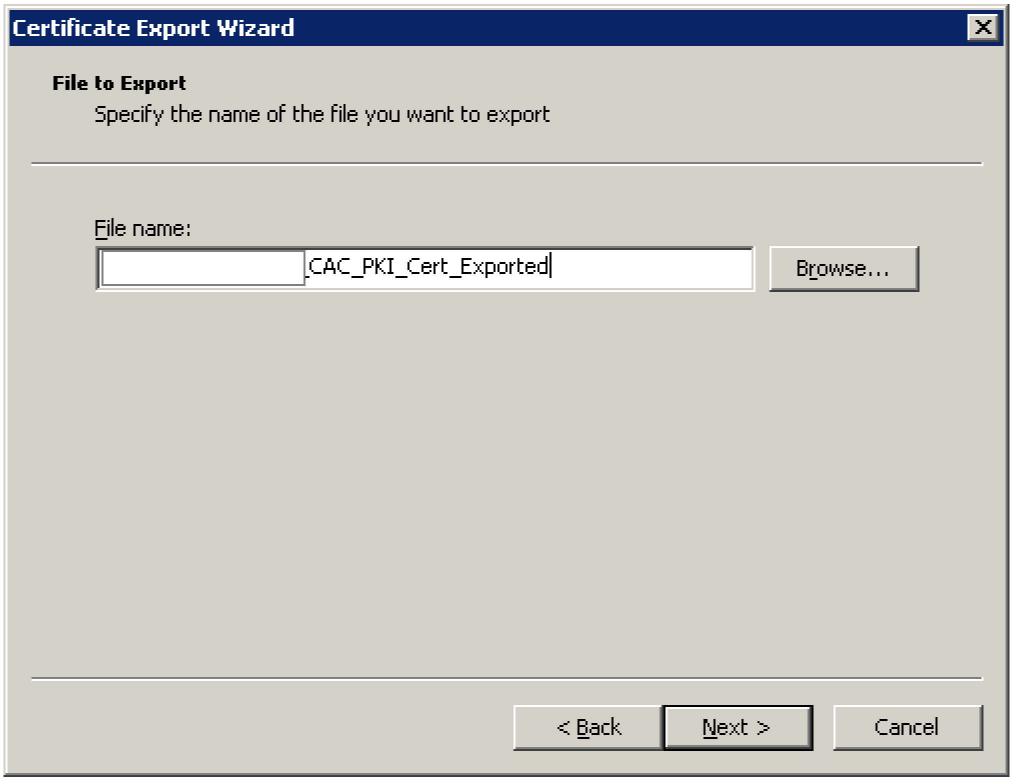
To maintain security, you must protect the private key by using a password.

Type and confirm a password.

Password: ●●●●●●●●●●●

Confirm password: ●●●●●●●●●●●

2.2.5. Choose a filename that makes sense



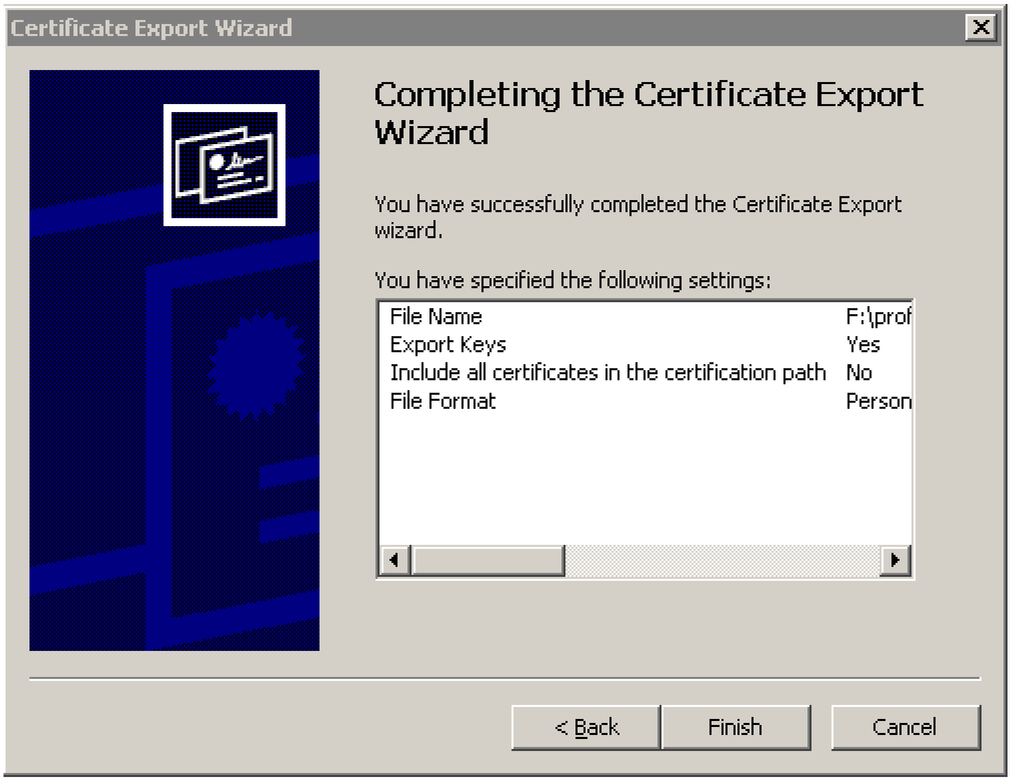
Certificate Export Wizard

File to Export

Specify the name of the file you want to export

File name: CAC_PKI_Cert_Exported

2.2.6. Click finish



Certificate Export Wizard

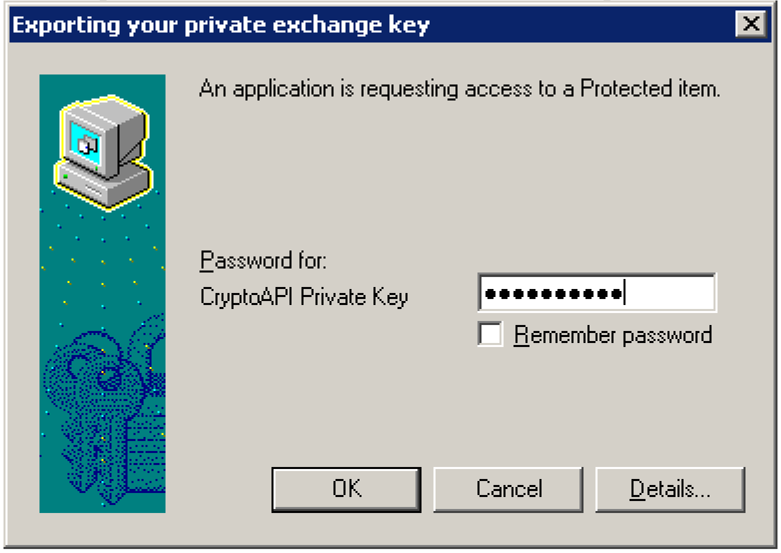
Completing the Certificate Export Wizard

You have successfully completed the Certificate Export wizard.

You have specified the following settings:

File Name	F:\prof
Export Keys	Yes
Include all certificates in the certification path	No
File Format	Person

2.2.7. Next, use the passphrase you used back in Step 19 of the AF PKI guide to import the DISA certificate into Internet Explorer



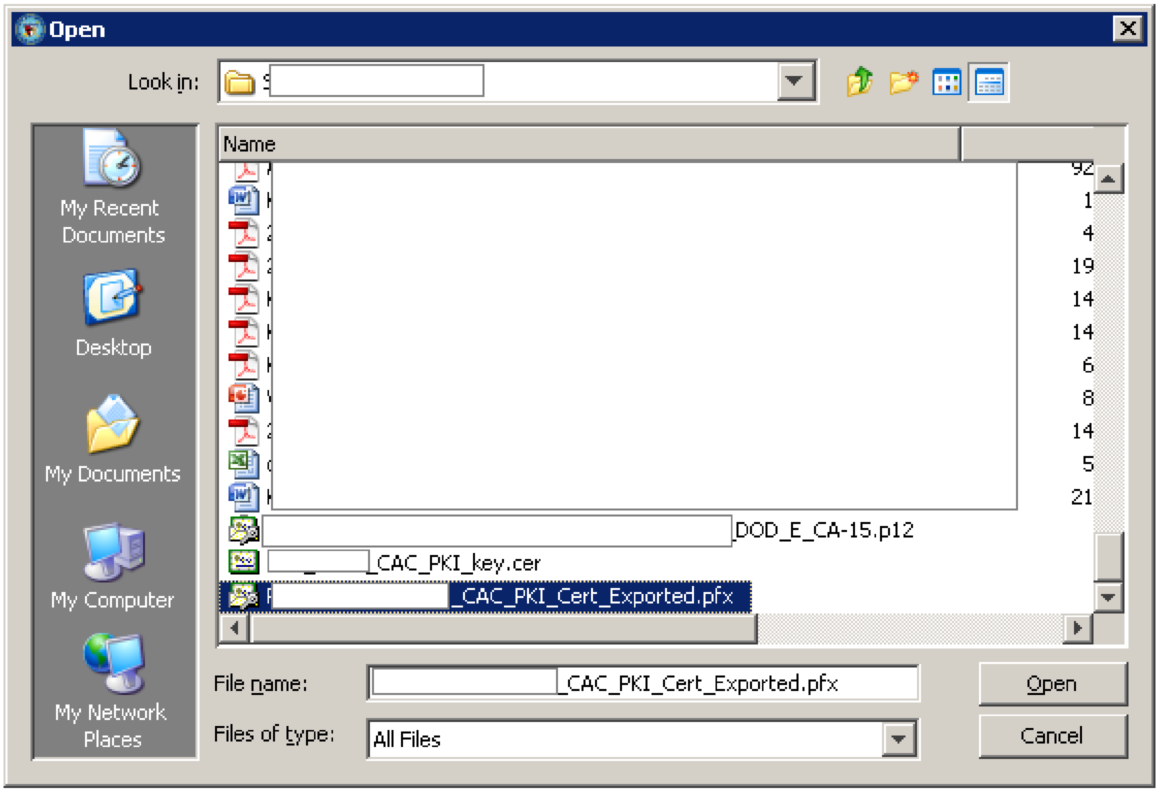
Exporting your private exchange key

An application is requesting access to a Protected item.

Password for:
CryptoAPI Private Key ●●●●●●●●●●●

□ Remember password

2.2.8. All Done



Look in: [redacted]

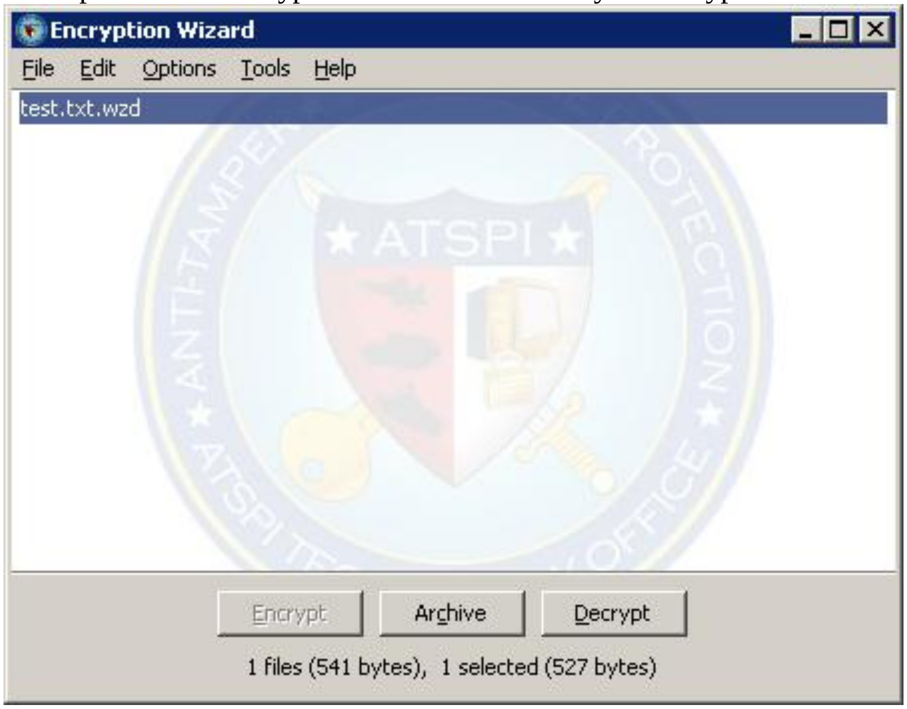
Name	
[redacted]	92
[redacted]	1
[redacted]	4
[redacted]	19
[redacted]	14
[redacted]	14
[redacted]	6
[redacted]	8
[redacted]	14
[redacted]	5
[redacted]	21
[redacted]DOD_E_CA-15.p12	
[redacted]_CAC_PKI_key.cer	
[redacted]_CAC_PKI_Cert_Exported.pfx	

File name: [redacted]_CAC_PKI_Cert_Exported.pfx

Files of type: All Files

3. Use exported PFX key with Encryption Wizard

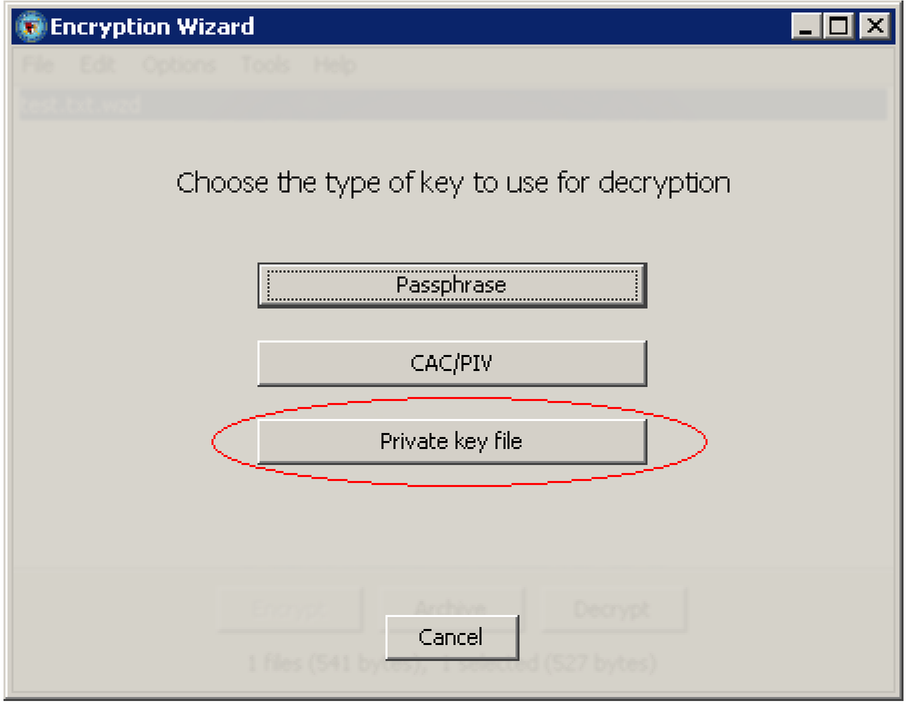
3.1. Open the file encrypted with the old PKI key in Encryption Wizard



test.txt.wzd

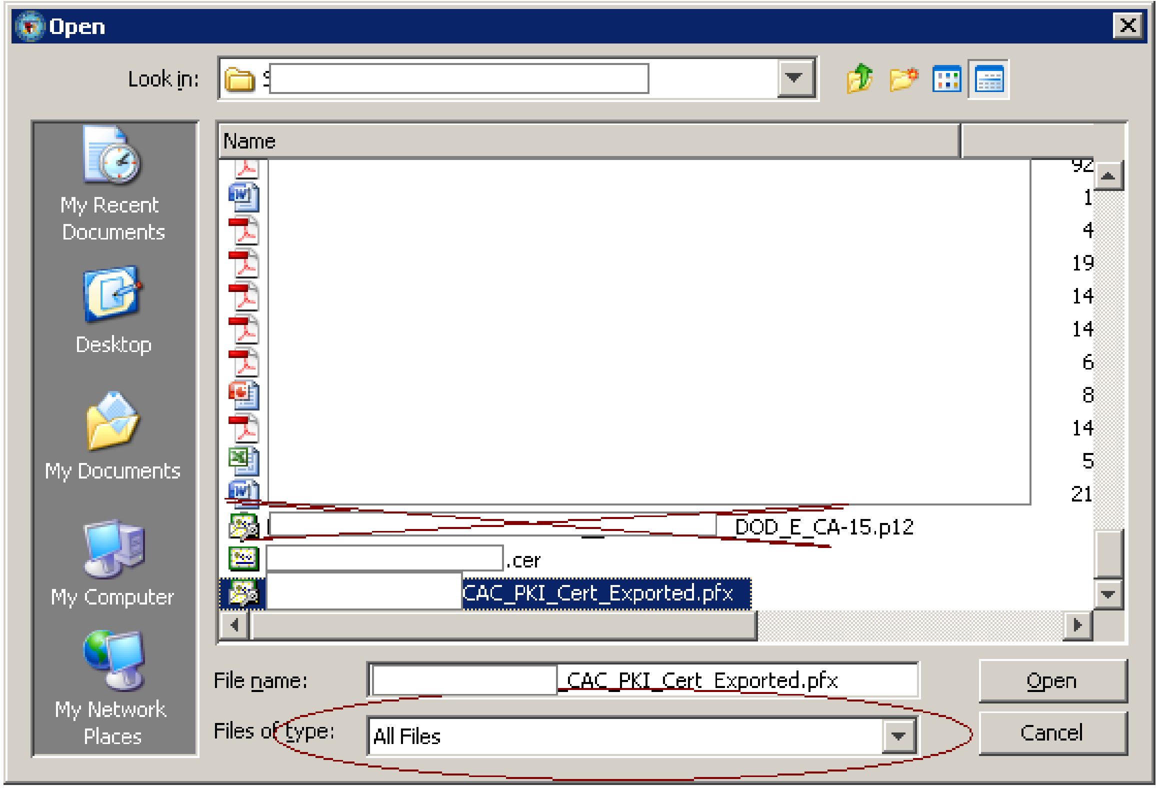
1 files (541 bytes), 1 selected (527 bytes)

3.2. Select “Decrypt”; select “Private key file”



Choose the type of key to use for decryption

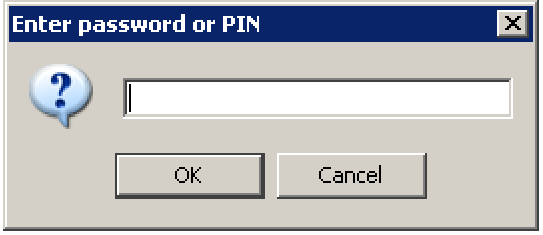
3.3. Select the PFX file exported in step 2.2.5 (**NOTE:** you need to expand the file selection filter to “all files” – not just “`.p12`” files)



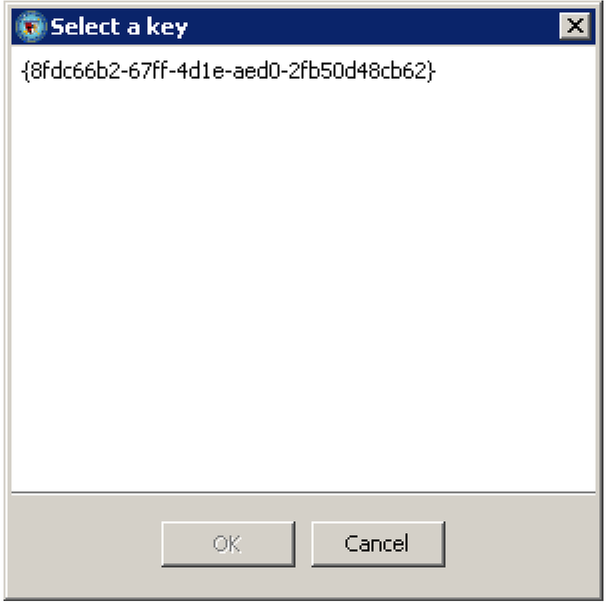
File name: CAC_PKI_Cert_Exported.pfx

Files of type: All Files

3.4. Enter password you selected in step 2.2.4.

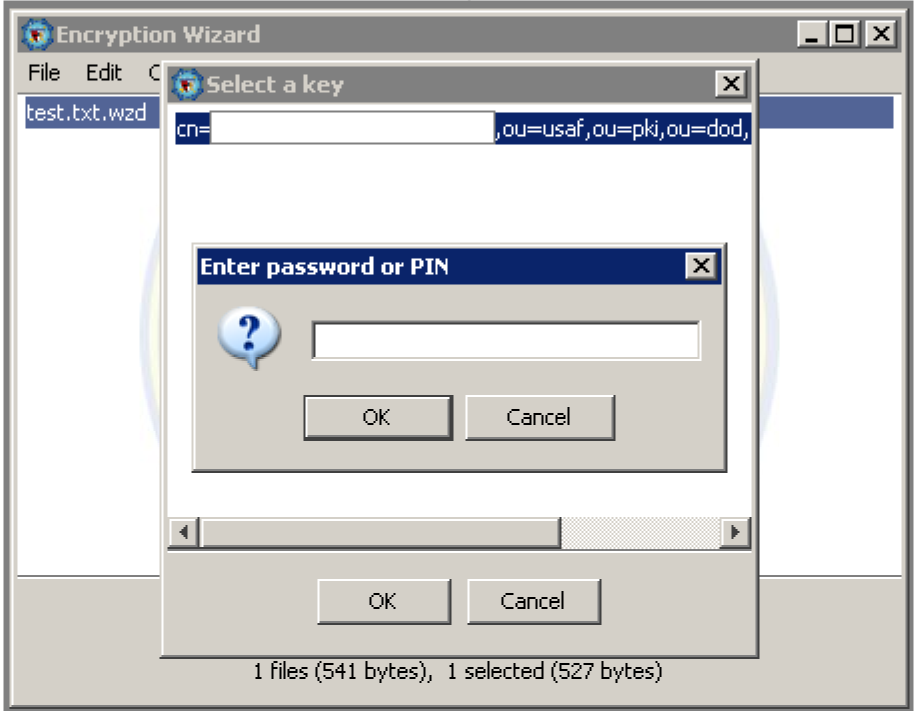


3.5. Select the key and press “OK”



{8fdc66b2-67ff-4d1e-aed0-2fb50d48cb62}

3.6. Enter password from step 2.2.4 again



cn=[redacted],ou=usaf,ou=pki,ou=dod,

1 files (541 bytes), 1 selected (527 bytes)

3.7. Continue using Encryption Wizard